The Wireless Threat

Wireless solves the access problem, enabling those with nefarious intentions to get into your system. Once inside, they can steal information, manipulate data, destroy data, or use your system to commit criminal acts. We worry about the ***insider threat***, but achieving access via wireless means gives hostile individuals remote, or virtual, access, obviating the need to have a physical presence within your spaces.

Four areas come to mind when considering the wireless threat – Local Area Nets [LANs], Supervisory Control and Data Acquisition [SCADA[1]] systems, a relatively new area, Radio Frequency Identification [RFID] systems, and Personal Digital Assistants [PDAs]. Note that, for this discussion, we are addressing the newer wireless systems [e.g., Wi-Fi] that have relatively short ranges. We are not considering the more traditional radio communications systems, such as satellite systems, cell phones and pagers, and air traffic control radars, which operate over long distances.

LANs

The new wireless LAN systems provide many advantages, most notably allowing users to access the LAN from mobile platforms. But, as with many technological advantages, it's a double-edged sword – there is a dark side. In this case, easy access for authorized users also means potentially easy access for unauthorized users.

This threat is real – consider these examples:

- In November 2001, a survey of London's financial center showed that numerous networks were accessible using a laptop in a car. More than two-thirds of the systems were not protected by encryption.[i]

- A survey of Manhattan showed more dramatic results. Using a few hundred dollars worth of hardware, a "war driving" survey accessed multiple access points within minutes, 79% of which had no encryption. What's more, the survey showed networks that were at least six blocks away could be accessed, far more than the few hundred meters often assumed. Access points were also found driving along Highway 101 in Silicon Valley at 60 mph.[ii]

- The FBI has discovered a systematic effort to mark physically unsecured wireless access points in major metropolitan areas – and activity dubbed "warchalking". It is akin to hobos marking places willing to give them a free meal, or spies marking "dead drop" locations for exchanging materials. Web sites are being used to

[1] A SCADA system is an industrial measurement and control system consisting of a central master station; one or more field data gathering and control units; and, a collection of standard or custom software used to monitor and control electromechanical devices, such as switches, pumps and valves. Often the devices are remote from the master station. SCADA systems are used in industrial processes, such as in refineries, electrical power generation, telecommunications, transportation, and flood control.

provide interactive digital maps denoting access points. This access threat has criminal, counterintelligence and counterterrorism implications, enabling access for data corruption or theft, anonymous criminal activity and cyber attack.[iii]

The National Institute of Standards and Technology [NIST] has been addressing these issues for the US Government.[iv] They provide a taxonomy for the threat; see Figure 1.

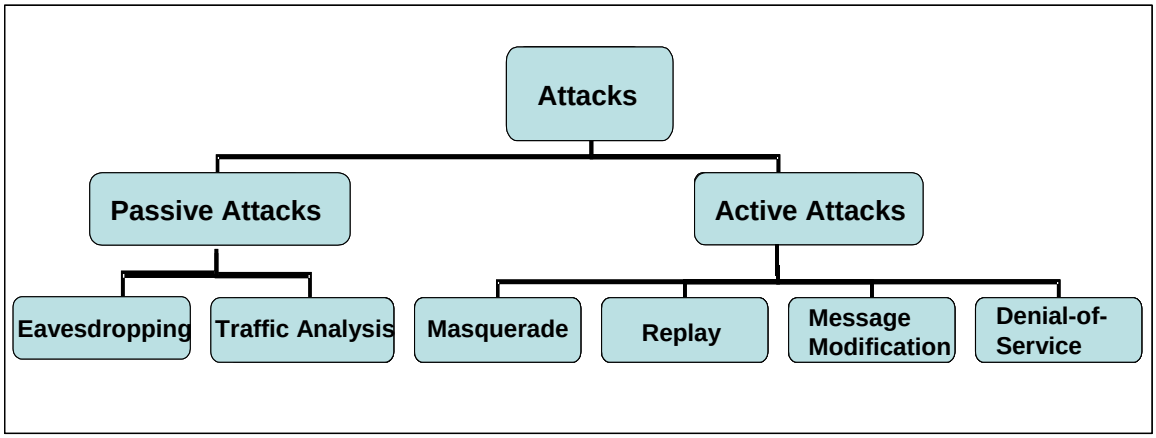

Figure 1 Taxonomy of Wireless LAN Attacks[v]

NIST defines the six attack types as follows:

- **"Passive Attack**—An attack in which an unauthorized party gains access to an asset and does not modify its content (i.e., eavesdropping). Passive attacks can be either eavesdropping or traffic analysis (sometimes called traffic flow analysis). These two passive attacks are described below.
  - **Eavesdropping**—The attacker monitors transmissions for message content. An example of this attack is a person listening into the transmissions on a LAN between two workstations or tuning into transmissions between a wireless handset and a base station.
  - **Traffic analysis**—The attacker, in a more subtle way, gains intelligence by monitoring the transmissions for patterns of communication. A considerable amount of information is contained in the flow of messages between communicating parties.

- **Active Attack**—An attack whereby an unauthorized party makes modifications to a message, data stream, or file. It is possible to detect this type of attack but it may not be preventable. Active attacks may take the form of one of four types (or combination thereof): masquerading, replay, message modification, and denial-of-service (DoS). These attacks are defined below.
  - **Masquerading**—The attacker impersonates an authorized user and thereby gains certain unauthorized privileges.

- **Replay**—The attacker monitors transmissions (passive attack) and retransmits messages as the legitimate user.
- **Message modification**—The attacker alters a legitimate message by deleting, adding to, changing, or reordering it.
- **Denial-of-service**—The attacker prevents or prohibits the normal use or management of communications facilities."[vi]

They note that: "The consequences of these attacks include, but are not limited to, loss of proprietary information, legal and recovery costs, tarnished image, and loss of network service."[vii]

NIST also notes that "some of these risks are similar to those of wired networks; some are exacerbated by wireless connectivity; some are new. Perhaps the most significant source of risks in wireless networks is that the technology's underlying communications medium, the airwave, is open to intruders…"[viii]

NIST provides a comprehensive checklist of security recommendations. The following is a short list of the more salient ones, which often are noted in other publications:

- Implement a security policy for wireless systems
- Stay abreast of and install all available security patches ASAP
- Deploy physical access controls, such as biometrics, to restrict access to authorized individuals
- Locate access points as far away as possible from the site exterior
- Run "red team" attacks against your system
- Use encryption
- Change the default Secure Service Indicator [SSID], and use a non-obvious one [i.e., don't use the company name, department, product name, etc.]
- Use firewalls and antivirus protection
- Ensure only authorized wireless devices can connect to the system
- Use strong passwords
- Employ network intrusion detection and auditing

Other suggested security measures include[ix, x]:

- Do not allow Administrator access via wireless access
- Periodically change encryption keys
- If data sensitivity warrants the expense of the best security, implement a Virtual Private Network [VPN]

As with all aspects of security, constant vigilance and dedicated personnel are key. Assign responsibility for wireless LAN security to trusted, knowledgeable individuals with the necessary resources and management backing.

<u>SCADA Systems</u>

It has been asserted that SCADA systems were not designed with security in mind. Indeed, their very nature – using wireless transmission and Internet links – makes security difficult.[xi] The double-edged sword rears its head again here – the attributes of being able to run remote diagnostics and update software, as well as monitor systems from a central location, also provide the easy access for hostile individuals.

As with LANs, there are horror stories to make the point:

- A cybersecurity firm survey of a large utility revealed one could connect wirelessly to the SCADA system within five minutes from a vehicle near a remote substation. They went on to map the entire network and then proceeded to access the business network, downloading several documents, within 20 minutes.[xii]

- In September 2002, a disgruntled job applicant attacked, from his car, a sewage control system in Australia, dumping millions of liters of raw sewage into the environment. He was captured and sent to prison.[xiii]

- Water utility executives reportedly have been alerted by the FBI that Osama bin Laden's terrorist network has researched their systems on the Web. Some have removed information on their SCADA systems from their websites, and others have added security upgrades. Another concern is the possibility of jamming the wireless SCADA systems of utilities.[xiv]

In many respects, the array of vulnerabilities and protective measures that apply to LANs also apply to SCADA systems. SCADA systems present the additional challenges of often having remote, unattended components, and posing potentially disastrous consequences if compromised. Some pumps, valves and breakers now come with their own plug-in SCADA connections[xv], providing potentially easy access at remote locations. SCADA systems may require a multiple "rings of defense" approach[xvi], involving a complementary combination of firewalls, encryption, network segmentation, separate passwords for each operator [and not a Post-it stuck to a monitor!], and supporting policies and procedures. The President's Critical Infrastructure Protection Board and the Department of Energy have published "21 Steps to Improve Cyber Security of SCADA Networks", addressing essential actions under two categories – implementation, and underlying management and policies.[xvii] Security professionals should consider reviewing this publication at www.ea.doe.gov/pdfs/21stepsbooklet.pdf.

<u>RFID</u>

RFID is the interactive version of the ubiquitous Universal Bar Code. It is just making its presence known in the commercial world, but portends an enormous impact as it permeates society. These systems consist of an RFID tag – containing a chip and an antenna – and a reader to interrogate the tag, along with the expected computer system. See Figures 2 and 3.

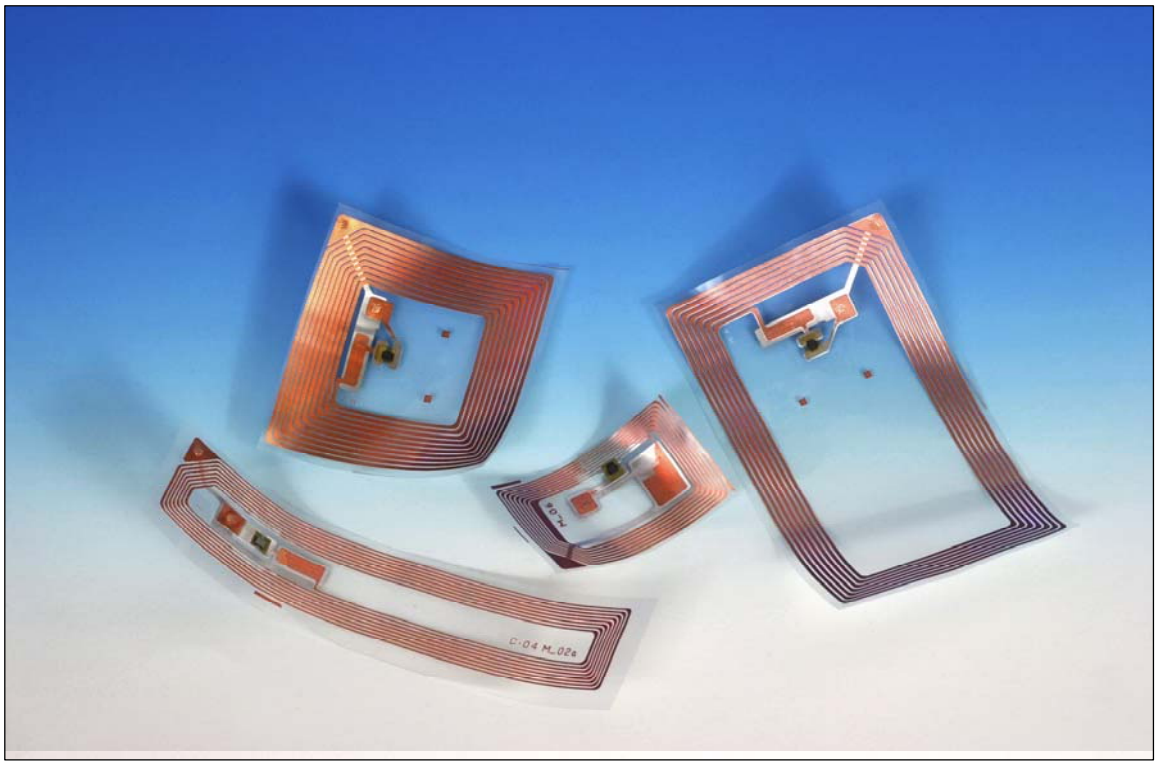

Figure 2 Texas Instruments RFID Tags[xviii]

As identification mechanisms, RFID systems offer several new attributes – they are non-contact, they are non-line-of-sight, the tags are passive, they enable 24x7 monitoring, the readers can be fixed or mobile, and the tags are so small they are easily surreptitious.[xix]

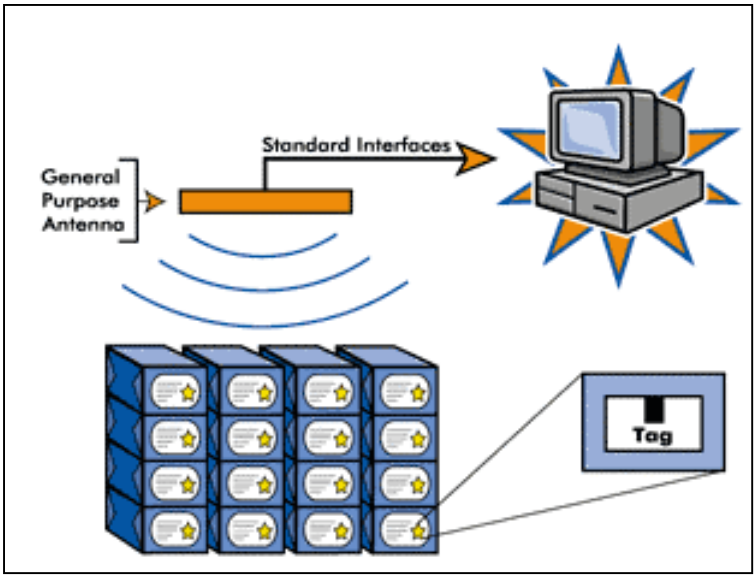

Figure 3 Illustrative RFID System[xx]

Here are some examples of current and planned RFID applications:

- Refrigerators that read RFID tags of their contents and alert owners that supplies are low or out-of-date
- An Italian washing machine that reads care instructions from an RFID tags in clothing
- Protective tags on museum works of art
- Badges for screening and tracking attendees at conferences [including the Academy Awards], and for employee access control
- Tracking grocery items as they are placed in the shopping cart[xxi], and for automated checkout
- Seals of authenticity in documents, designer products and currency to discourage counterfeiting[xxii]
- EZ Pass car toll payment systems and Speed Pass gasoline purchase systems[xxiii]
- Smart passes for the Washington, DC, Metro and London Underground
- Organizers of the 2006 FIFA World Cup soccer games in Germany plan to issue tickets with smart tags[xxiv]
- By far the biggest near-term market seems to be in the retail inventory control/supply chain area
    - Wal-Mart is requiring its top 100 suppliers to have RFID labels at the case and pallet level by January 2005
    - Gillette plans to put RFID tags on razor blades
    - Canon USA wants to put them on its printers and copiers
    - The US Postal Service is investigating putting them on pieces of mail
    - Gap has tested them on denim clothes for both inventory control and ease of finding a particular item in a store[xxv]

The security implications of RFID are probably only just being addressed. The privacy concerns are profound. The ability to track people in terms of their locations and movements, as well as their purchasing habits has privacy activists alarmed. But, from an organizational perspective, the prospects for corporate or other nefarious spying on inventories, personnel monitoring, tracking of individuals and unwitting tagging all raise security and counterintelligence concerns. Thus, as with the LANs and SCADA systems, system access, data security and vulnerability to denial of service attacks must all be considered. Encryption will present a severe challenge, given the desire to make the tags as low cost as possible for large commercial applications.[xxvi] Figure 4 shows how small the RFID components can be.

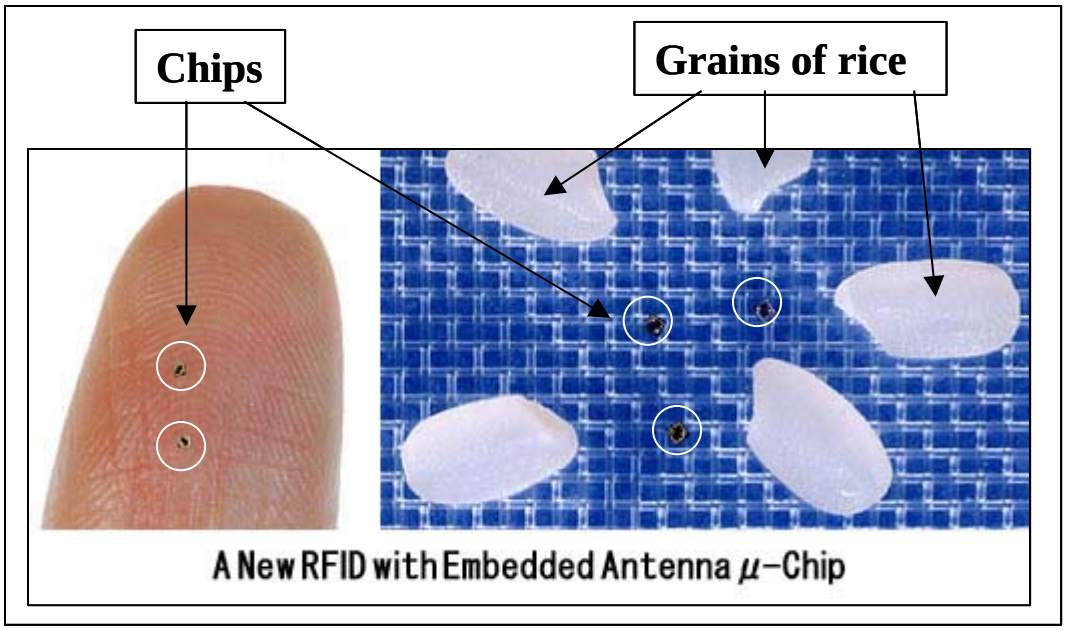

Figure 4 Hitachi's New 0.4x0.4 mm RFID Chip[xxvii]

PDAs

PDAs have a dual threat associated with them -- their access to a network provides an entry point to attack the network, plus they can be targets themselves because they store data. And, their small size makes them easy to be stolen, misplaced or lost.[xxviii]

PDAs can provide access to networks via a wire connection, an infrared communications port, or a wireless radio connection. PDA users connect to networked computers to backup data to the desktop computer, or download data or application programs from the desktop computer.[xxix] The mirroring of data between the PDA and the desktop computer is called "syncing". The ease with which PDAs can access LANs provides the holder of a stolen PDA a convenient tool to attempt, and probably effect, network access.

PDAs also have several unique vulnerabilities:

- They are susceptible to the introduction of viruses, for example through wireless RF or IR communications ports, or through Internet connectivity that enables receipt of e-mails. In turn, the PDA can pass a virus on to other PDAs or its owner's network.[xxx] Three PDA viruses have been noted -- all directed at Palms
  - Liberty Crack, a Trojan Horse virus that deletes all files not preloaded on the PDA
  - Vapor, which makes all application icons disappear
  - Phage, which targets wireless PDAs, which also attacks all non-preloaded programs[xxxi]
- Some PDAs have a built-in voice recording capability. This can be unintentionally activated and thus record conversations.[xxxii]

- Many PDA users store business contact information, passwords and PINs, bank account data and corporate information on their PDAs.[xxxiii] Clearly the loss of such data, either by physical loss of the device or via someone accessing the PDA via its remote ports, makes the data vulnerable.

Several groups[xxxiv] have studied the security aspects of PDAs. The more salient of their recommendations that are unique to PDAs follow:

- Manage the devices in terms of personnel possession, network access, Internet Service Providers [ISPs] subscribed to by users, and software put on the devices
- Activate and use access control features, especially passwords and PINs, which should be changed regularly
- Use encryption [although this is limited by the capability of the device]
- Use anti-virus protection
- Do not allow PDAs in sensitive areas [because of the ease with which they can connect to networks as well as the recording feature on some devices]
- Do not grant access to classified networks

Although PDAs are not as widespread as PCs, they are proliferating. Recent sales levels average about ten million units per year, about half of these in the US.[xxxv] So, the problem can only get worse in the future.[xxxvi]

Risk Mitigation

Risk mitigation always involves a cost tradeoff. The amount of mitigation, of course, should be commensurate with the value of the information being protected. NIST breaks risk mitigation measures into three areas – management, operational and technical.

- Management countermeasures involve development and implementation of a security policy and personnel training.
- Operational countermeasures involve physical security measures, such as personnel access controls, location of equipment and boundary protection.
- Technical countermeasures involve the use of the panoply of hardware and software security measures that are available. Here is where choices that weigh costs come most into play.

Final Thoughts

Those with responsibility for acquiring or using wireless LANs, SCADA systems or RFID systems will be faced with security challenges. Personnel will have to be dedicated with keeping up to date on a range of fast-changing security issues, such as encryption, standards, patches and protocols, as well as evolving technology trends.

[i] "Is Wireless Internet Safe to Use?, Eric Byres and Gordon Gillespie, www.sensormag.com, July 2002
[ii] Exploiting and Protecting 802.11b Wireless Networks, Craig Ellison, www.extremetech.com, September 4, 2001
[iii] New Risk for Wireless Access Points; Warchalkers marking WiFi sites, Feds warn, Computerworld, August 19, 2002
[iv] Wireless Network Security, by Tom Karygiannis and Les Owens, NIST Special Publication 800-48, November 2002
[v] Ibid.
[vi] Ibid.
[vii] Ibid.
[viii] Ibid, p ES-1
[ix] Securing Your Wireless Network, www.practicallynetworked.com/support/wireless_secure.htm
[x] Ellison, Op.Cit.
[xi] SCADA vs. the hackers, Alan S. Brown, Mechanical Engineering Magazine, December 2002
[xii] Ibid.
[xiii] Byres and Gillespie, Op. Cit.
[xiv] Water Systems Improve Net Security After FBI Warning; Wireless systems vulnerable to jams, Bob Brewin, Computerworld, March 4, 2002
[xv] Brown, Op.Cit.
[xvi] SCADA Security Strategy, Jonathan Pollet, PlantData Technologies, August 8, 2002
[xvii] At www.ea.doe.gov/pdfs/21stepsbooklet.pdf
[xviii] www.ti.com
[xix] Get Ready! Wal-Mart Mandate Puts RFID, Smart Tags On Fast Track, Jean V. Murphy, SupplyChainBrain.com, September 2003
[xx] www.matrics.com
[xxi] RFID Tags and the Question for Personal Privacy, Jack M. Germain, TechNewsWorld, November 18, 2003
[xxii] RFID Systems and Security and Privacy Implications, Sanjay E. Sarma, Stephen A. Weis, and Daniel W. Engels, Auto-ID Center, MIT, undated
[xxiii] Germain, Op.Cit.
[xxiv] Big play on RFID at German world soccer cup, John Blau, IDG News Service, Düsseldorf Bureau, 16-01-2004
[xxv] A Radio Chip in Every Consumer Product, Claudia H. Deutsch and Barnaby J. Feder, New York Times, February 25, 2003
[xxvi] Sarma et al, Op. Cit.
[xxvii] www.hitachi.com/New/cnews/030902.html
[xxviii] Karygiannis and Owens, Op.Cit.
[xxix] Symantec Corporation, Threats to PDAs, at www.symantec.com/avcenter/reference/malicious.threats.to.pdas.html
[xxx] Palms Ripe for Bug Attacks, Maria Godoy, TechTV News, May 23, 2001
[xxxi] The Emerging Threat of PDA Viruses, Jessica Lee, Nicholas Idler, Matthew Gundersen and Krista Casady, Geek.com, May 8, 2001
[xxxii] Personal Digital Assistant Vulnerability Assessment, Government of Canada, Communications Security Establishment, ITSPSR-18, October 2002
[xxxiii] Securing the PDA, Brian Betts, Techworld, at computercops.biz
[xxxiv] Government of Canada, Op.Cit.; Karygiannis and Owens, Op.Cit.; Wireless PDAs and Security, Kasten Chase, The President's National Security Telecommunications Advisory Committee [NSTAC] Wireless Task Force, October 8,2002; Symantec, Op.Cit.; Ten Tips to Combat Handheld Attacks, Bluefire Security Technologies [as quoted at www.smartphonetoday.com]
[xxxv] PDA Sales Steer Steady Course, Amy Gilroy, November 24, 2003, at www.wirelessweek.com
[xxxvi] Godoy, Op.Cit.